## REMARKS

This Amendment is in response to the Office Action mailed June 17, 2004. The Office Action rejected claims 1-17 under 35 U.S.C. § 102(e).

Claims 1 and 15 have been amended. Claim 18 has been added. Claims 1-18 remain pending in the application. No claims have been cancelled. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

**Priority**

In compliance with 35 U.S.C. 119(b), Applicants herewith submit a certified copy of Japanese patent application 11-099657 on which priority is claimed.

**Rejections Under 35 U.S.C. § 102(e)**

The Office Action rejected claims 1-17 under 35 U.S.C. § 102(e) as being anticipated by Sabin et al. (U.S. Patent No. 6,026,421).

Claims 1 and 15 of the present patent application are directed to a multi-word arithmetic device for executing modular arithmetic on multi-word integers. These claims include the limitations of:

"an arithmetic unit for executing, on word units, at least two types of word calculations, including addition and multiplication, and outputting a one-word calculation result", and

"a memory input/output circuit for performing (1) a first data transfer for storing in the memory at least one integer received from an external device, (2) a second data transfer for inputting at least one integer stored in the memory into the arithmetic unit in word units, (3) a third data transfer for storing in the memory the calculation result output from the arithmetic

unit, and (4) a fourth data transfer for outputting the calculation result from the memory to the external device" and

"a control circuit for .... when the selected modular arithmetic is performed, the control circuit repeatedly instructs, for each word of the at least one integer, the arithmetic unit to perform the word calculation."

With provision of one arithmetic unit and the control circuit as above, the multi-word arithmetic device achieves an effect that modular arithmetic on multi-word integers can be performed without requiring larger-scale hardware. For example, the multi-word arithmetic device of the present invention may be applied to an encryption apparatus. Generally, in order to ensure the security in secret communications, an encryption apparatus is required to compute a long-word integer, 2,048 bits, for example. In the case of the multi-word arithmetic device of the present invention, such a long-word integer can be computed with one 32-bit arithmetic unit. Here, the control circuit repeatedly instructs the arithmetic unit to perform the word calculation on each word that together makes up that long-word integer. With this structure, even when processing a long-word integer, it is not necessary to use large-scale hardware.

The Sabin reference discloses a technique for performing multiplication and modular reduction of large integers. Fig. 3 of the Sabin reference shows four large integer units (LIUs). Each word of a large integer is associated with one of the four LIUs and the word is computed by an associated LIU. Thus, the Sabin reference requires a plurality of LIUs for computing a large integer. With this structure, in order to compute an integer having a longer word-length, the resulting circuitry needs to be inevitably larger. Unlike the present claimed invention, the size of the large-word integer operations that can be computed using the structure taught by Sabin is

limited by the number of LIUs. By contrast, the present claimed invention includes a control circuit (not disclosed by Sabin) which enables the present claimed invention to perform large-word integer operations without the need for more arithmetic units. That is, the present claimed structure can perform arithmetic operations on larger word integers because the control circuit "instructs, for each word of the at least one integer, the arithmetic unit to perform the word calculation."

Thus, the present invention eliminates the need for the larger-scaled circuitry (taught by Sabin) when an integer having a longer word-length is computed.

For the above reasons, Applicants submit that independent claims 1 and 15, and all of their dependent claims are patentably distinct from Sabin and are in condition of allowance.

## Conclusion

In view of the amendments and remarks made above, it is respectfully submitted that the pending claims are in condition for allowance, and such action is respectfully solicited. Authorization is hereby given to charge our Deposit Account No. 19-2814 for any charges that may be due. Furthermore, if an extension is required, then Applicants hereby request such an extension.

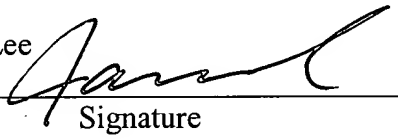
Respectfully submitted,

Snell & Wilmer, L.L.P.

Julio Loza
Registration. No. 47,758
SNELL & WILMER L.L.P.
1920 Main St., Suite 1200
Irvine, CA 92614
Telephone: (949) 253-4924

I hereby certify that this document and fee is being deposited on September 17, 2004 with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the MAIL STOP AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313

By: James Lee



Signature

Dated: September 17, 2004